UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/908,656	06/03/2013	Jeff P. Kendrick	PROP 0102 PUS2	2667

22045 7590 07/26/2017

BROOKS KUSHMAN P.C.
1000 TOWN CENTER
TWENTY-SECOND FLOOR
SOUTHFIELD, MI 48075

EXAMINER	
DONLON, RYAN D	

ART UNIT	PAPER NUMBER
3695	

NOTIFICATION DATE	DELIVERY MODE
07/26/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@brookskushman.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte JEFF P. KENDRICK,
FRANK ANTHONY ALLEN,
PAUL HAROLD ANDERSON,
and WAYNE WILLIAM PECK

Appeal 2015-005522
Application 13/908,656
Technology Center 3600

Before ANTON W. FETTING, NINA L. MEDLOCK, and
AMEE A. SHAH, *Administrative Patent Judges.*

FETTING, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE[1]

Jeff P. Kendrick, Frank Anthony Allen, Paul Harold Anderson, and Wayne William Peck (Appellants) seek review under 35 U.S.C. § 134 of a

---

[1] Our decision will make reference to the Appellants' Appeal Brief ("App. Br.," filed December 16, 2014) and Reply Brief ("Reply Br.," filed May 4, 2015), and the Examiner's Answer ("Ans.," mailed March 3, 2015), and Final Action ("Final Act.," mailed July 16, 2014).

final rejection of claims 1–4 and 9–11, the only claims pending in the application on appeal. We have jurisdiction over the appeal pursuant to 35 U.S.C. § 6(b).

The Appellants invented a way to allow merchants to perform payment processing such that the merchant is only required to identify a unique identifier of a customer account and not data specific to a particular payment device. Specification para. 2.

An understanding of the invention can be derived from a reading of exemplary claim 1, which is reproduced below (bracketed matter and some paragraphing added).

1. A method of

processing electronic payment transactions

using at least one payment device of a customer

without requiring a merchant to store sensitive data

specific to the at least one payment device,

the method comprising:

[1] receiving a notification from a merchant

that a customer is attempting an electronic payment transaction at a secure payment system,

the secure payment system including one or more servers that include one or more processors and one or more storage devices;

[2] determining by the secure payment system

that the electronic payment transaction requires sensitive data

that when stored by the merchant imposes regulations on the merchant

to protect the sensitive data,

wherein the regulations includes standards

relating to the security of the sensitive data stored in the secure payment system;

[3] receiving identification information of a customer account

while the customer is attempting the electronic payment transaction;

[4] generating a unique identifier associated with the customer account;

[5] receiving sensitive data

specific to a first payment device

from the customer

while the customer is attempting the electronic payment transaction

such that the merchant does not store the sensitive data specific to the first payment device;

[6] storing identification information of

the customer account

and

the sensitive data specific to the first payment device;

[7] providing the unique identifier

to at least one of the merchant or a customer;

[8] receiving a payment processing request from the merchant

that includes the unique identifier

and not the sensitive data specific to the first payment device;

and

[9] processing the payment processing request

using the first payment device

such that the merchant is only required to identify the unique identifier of the customer account

> and not the sensitive data specific to the first payment device.

The Examiner relies upon the following prior art:

Singhal	US 2002/0062281 A1	May 23, 2002
Gupta	US 2006/0064372 A1	Mar. 23, 2006

Hall, *A Stolen Identity Will Cost You*, Air Conditioning, Heating & Refrigeration News, vol. 230, iss. 7, p. 1 (Feb. 12, 2007) ("Hall").[2]

Claims 1–4 and 9–11 stand rejected under 35 U.S.C. § 101 as directed to non-statutory subject matter.

Claims 1–4 and 9–11 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Gupta, Singhal, and Hall.

ISSUES

The issues of eligible subject matter turn primarily on whether the claims are directed to more than conceptual advice of what data to provide. The issues of obviousness turn primarily on whether the prior art suggests applying the modifications in Singhal to Gupta.

---

[2] The Examiner erroneously lists the title as "NeoScale Extends Storage Security Leadership." Both articles were included in the same file listed on the Notice of References Cited mailed April 3, 2014. The proper title and article is the second article in that file.

FACTS PERTINENT TO THE ISSUES

The following enumerated Findings of Fact (FF) are believed to be supported by a preponderance of the evidence.

Facts Related to the Prior Art

Gupta

01. Gupta is directed to facilitating selective use of two or more accounts associated with a single transaction account identifier. Gupta para. 1.

02. Gupta describes a common transaction account identifier that can be used in transactions associated with one of multiple transaction accounts. Gupta includes one or more of the following steps: establishing at least two transaction accounts, wherein the transaction accounts are respectively associated with transaction account identifiers (e.g., numbers, letters, symbols, signals and/or the like); receiving, at a transaction processing system, a common account identifier; recognizing the common account identifier as being associated with more than one account; and determining which of the at least two transaction accounts to access for processing the transaction. The determining step may be based on selection criteria, and the selection criteria may be modified by a user of the first and second transaction accounts. One of the first and second transaction account identifiers may be forwarded to the respective first and second transaction accounts based on the determining step; and the transaction may be processed via the selected transaction account. Gupta para. 5.

03. Gupta uses its card in card readers for payments to merchants. Gupta para. 18.

04. Gupta associates its card with a common account identifier/card number. Furthermore, an "account identifier", "card number", "code", "identifier" or "loyalty number" may include any device, code, or other identifier/indicia suitably configured to allow the consumer to interact or communicate with the system, such as, for example, authorization/access code, personal identification number (PIN), Internet code, other identification code, and/or the like that is optionally located on a rewards card, pre-paid card, telephone card, smart card, magnetic stripe card, bar code card, radio frequency card and/or the like. The account identifier may be distributed and stored in any form of plastic, electronic, magnetic, radio frequency, audio and/or optical device capable of transmitting or downloading data from itself to a second device. An account identifier may be, for example, a sixteen-digit card number, although each card provider has its own numbering system, such as the fifteen-digit numbering system used by an exemplary loyalty system. Each company's card numbers comply with that company's standardized format such that the company using a sixteen-digit format may generally use four spaced sets of numbers, as represented by the number "0000 0000 0000 0000". The first five to seven digits are reserved for processing purposes and identify the issuing bank, card type, etc. In this example, the sixteenth digit is used as a sum check for the sixteen-digit number.

The intermediary eight-to-ten digits are used to uniquely identify the customer. In addition, loyalty account identifiers of various types may be used. Gupta para. 20.

Singhal

05. Singhal is directed to facilitating private and secure payment transactions between a customer and a merchant and between private parties. Singhal para. 5.

06. Singhal describes a customer not having to share his/her identity, personal sensitive data, and purchasing habits with the merchants and the banks. Singhal para. 15.

07. When the customer is using the payment card at the location of the merchant, the payment card can be swiped in a card reader. A Card Personal Identification Number (CPIN) is entered into the card reader by the customer. The merchant identification and a payment amount is entered into the card reader by the merchant, and a data record including at least the foregoing data and the encrypted card number is transferred over the global network to the central system. The central system decrypts the payment card number to identify the customer identification. Figure 7C illustrates an approach of the Security Function that takes an encrypted card number and determines the customer identification. The card number along with its expiration date and a CPIN that is entered by the customer is received by the system. The 16 digits of the card number are parsed into four 4-digit numbers. In the security function, four offset numbers that

correspond to the 4-digit expiration date are read. The offset numbers are added to each of the four 4-digit numbers. The modified four 4-digit numbers are combined to form a customer identification number. Using the customer identification number and the CPIN from the customer database, the particular bankcard data, which the customer wishes to use for this payment transaction is obtained. Singhal paras. 69–70.

Hall

08. Hall is directed to the risks of failing to secure online private information. Hall Abstract.

ANALYSIS

Claims 1–4 and 9–11 rejected under 35 U.S.C. § 101 as directed to non–statutory subject matter

The Supreme Court

> set forth a framework for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts. First, [] determine whether the claims at issue are directed to one of those patent-ineligible concepts. [] If so, we then ask, "[w]hat else is there in the claims before us? [] To answer that question, [] consider the elements of each claim both individually and "as an ordered combination" to determine whether the additional elements "transform the nature of the claim" into a patent-eligible application. [The Court] described step two of this analysis as a search for an "'inventive concept'"—i.e., an element or combination of elements that is "sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself."

Alice Corp., Pty. Ltd. v. CLS Bank Int'l, 134 S. Ct. 2347, 2355 (2014) (citing *Mayo Collaborative Services v. Prometheus Labs, Inc.*, 132 S. Ct. 1289 (2012)).

To perform this test, we must first determine whether the claims at issue are directed to a patent-ineligible concept.

The Examiner finds the claims directed to electronic payment processing. Final Act. 2. Although this is so, there is an even more fundamental direction to these claims. The preamble to claim 1 recites that it is a method of processing electronic payment transactions using at least one payment device of a customer without requiring a merchant to store sensitive data specific to the at least one payment device. The steps in claim 1 result in making a payment without having to access privileged information. The Specification at paragraph 2 recites that the invention relates to allowing merchants to perform payment processing such that the merchant is only required to identify a unique identifier of a customer account and not data specific to a particular payment device. Thus, all this evidence shows that claim 2 is directed to storing sensitive data in such a way that it may be accessed without the merchant, i.e., information escrowing (sensitive information is held in escrow bypassing the merchant, and the escrow release is completed by providing the recited unique identifier).

It follows from prior Supreme Court cases, and *In re Bilski*, 545 F.3d 943 (Fed. Cir. 2008) in particular, that the claims at issue here are directed to an abstract idea. Like the risk hedging in *Bilski*, the concept of escrow is a fundamental business practice long prevalent in our system of commerce. The use of escrow is also a building block of property protection. Data escrow is now a long-used practice to protect both a security interest and

privacy interest held by different parties in the same data. Thus, data escrow, like hedging, is an "abstract idea" beyond the scope of §101. *See Alice Corp. Pty. Ltd.*. 134 S. Ct. at 2356.

As in *Alice Corp. Pty. Ltd.*, we need not labor to delimit the precise contours of the "abstract ideas" category in this case. It is enough to recognize that there is no meaningful distinction in the level of abstraction between the concept of risk hedging in *Bilski* and the concept of escrow at issue here. Both are squarely within the realm of "abstract ideas" as the Court has used that term. *See Alice Corp. Pty. Ltd.*, 134 S. Ct. at 2357.

Further, claims involving data collection, analysis, and display are directed to an abstract idea. *Elec. Power Grp. v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016) (holding that "collecting information, analyzing it, and displaying certain results of the collection and analysis" are "a familiar class of claims 'directed to' a patent ineligible concept"); *see also In re TLI Commc'ns LLC Patent Litig.*, 823 F.3d at 611; *FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089, 1093–94 (Fed. Cir. 2016). Claim 1, unlike the claims found non-abstract in prior cases, uses generic computer technology to perform data collection, analysis, and processing and does not recite an improvement to a particular computer technology. *See, e.g., McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1314–15 (Fed. Cir. 2016) (finding claims not abstract because they "focused on a specific asserted improvement in computer animation"). As such, claim 1 is directed to the abstract idea of receiving, analyzing, and processing data.

Claims 2–4 merely describe the data employed. We conclude that the claims at issue are directed to a patent-ineligible concept.

The introduction of a computer into the claims does not alter the analysis at *Mayo* step two.

> the mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention. Stating an abstract idea "while adding the words 'apply it'" is not enough for patent eligibility. Nor is limiting the use of an abstract idea "'to a particular technological environment.'" Stating an abstract idea while adding the words "apply it with a computer" simply combines those two steps, with the same deficient result. Thus, if a patent's recitation of a computer amounts to a mere instruction to "implement[t]" an abstract idea "on . . . a computer," that addition cannot impart patent eligibility. This conclusion accords with the preemption concern that undergirds our §101 jurisprudence. Given the ubiquity of computers, wholly generic computer implementation is not generally the sort of "additional feature[e]" that provides any "practical assurance that the process is more than a drafting effort designed to monopolize the [abstract idea] itself."

Alice Corp. Pty. Ltd., 134 S.Ct. at 2358 (citations omitted).

"[T]he relevant question is whether the claims here do more than simply instruct the practitioner to implement the abstract idea [] on a generic computer." *Alice Corp. Pty. Ltd.*, 134 S.Ct. at 2359. They do not.

Taking the claim elements separately, the function performed by the computer at each step of the process is purely conventional. Using a computer to receive data, determine what data is needed, generate data, store data, and process payments in the form of data amounts to electronic data query and retrieval—one of the most basic functions of a computer. All of these computer functions are well-understood, routine, conventional activities previously known to the industry. In short, each step does no more than require a generic computer to perform generic computer functions.

Considered as an ordered combination, the computer components of Appellants' method add nothing that is not already present when the steps are considered separately. Viewed as a whole, Appellants' method claims simply recite the concept of data escrow as performed by a generic computer. To be sure, the claims recite doing so by advising one to look at the data in a transaction to see if secure processing is needed and if so, generating identifier data, and using that identifier as a stand-in for data that need to be secured. But this is no more than abstract conceptual advice on the parameters for such escrow and the generic computer processes necessary to process those parameters, and does not recite any particular implementation. Even the step of "receiving sensitive data specific to a first payment device . . . such that the merchant does not store the sensitive data specific to the first payment device" is no more than abstract conceptual advice absent any implementation detail. As it is, the claim is little more than advising one to use an alias to hide sensitive information.

The method claims do not, for example, purport to improve the functioning of the computer itself. Nor do they effect an improvement in any other technology or technical field. The 25 pages of the Specification spell out different generic equipment and parameters that might be applied using this concept and the particular steps such conventional processing would entail based on the concept of escrowing data under different criteria. They do not describe any particular improvement in the manner a computer functions. Instead, the claims at issue amount to nothing significantly more than an instruction to apply the abstract idea of escrow using some unspecified, generic computer. Under our precedents, that is not enough to

transform an abstract idea into a patent-eligible invention. *See Alice Corp. Pty. Ltd.*, 134 S. Ct. at 2360.

As to the structural claims, they

> recite the abstract idea implemented on a generic computer; the system claims recite a handful of generic computer components configured to implement the same idea. This Court has long "warn[ed] ... against" interpreting § 101"in ways that make patent eligibility 'depend simply on the draftsman's art.'

Alice Corp. Pty. Ltd., 134 S. Ct. at 2360. Further, the structural claims are far more broad and abstract than claim 1. Claims 9 and 10 substitute an alias for an account number, and claim 11 also interprets the alias back to the account number. These claims do not even go so far as to escrow the data. There is little more abstract than substituting an alias for a name.

We are not persuaded by Appellants' argument that

> the claims are a technical solution to a technical problem. Put a different way, the challenge of creating infrastructure that would enable merchants to perform payment processing requests without being PCI[3]-compliant is not a mere fundamental economic practice of organizing human activities.

App. Br. 4. The claims are not a technical solution as they do nothing to the underlying technology. The claims do not mention the technical details of PCI compliant architecture, much less how the technology is changed to get around its requirements. Instead, the claims recite conceptual advice for substituting one name for another and depositing data.

---

[3] PCI ("Payment Card Industry")

Claims 1–4 and 9–11 rejected under 35 U.S.C. § 103(a) as unpatentable over Gupta, Singhal, and Hall

The Examiner applies Gupta for conventional payment processing and finds that Hall shows why it is important to protect private information in transactions such as in Gupta. The Examiner then applies Singhal to show it was known to provide an account number alias in the form of an encrypted customer identification and to protect private data by retaining it in a separate database.

We are not persuaded by Appellants' argument that the Examiner's reasoning for combining the references was conclusory. App. Br. 4–5. Although the Examiner did find that Gupta was ready for improvement, this was with respect to the warning in Hall that the data in Gupta needed protection. The Examiner does conclude the result would have been predictable, but this is more of a statement of the predictability of the art after finding that Singhal provided a mechanism for improving on Gupta for the reasons articulated in Singhal (a customer not having to share his/her identity, personal sensitive data).

Appellants argue that the art does not describe receiving sensitive data specific to a first payment device from the customer while the customer is attempting the electronic payment transaction such that the merchant does not store the sensitive data specific to the first payment device. Reply Br. 2–3. This argument is untimely as it was not presented in the Appeal Brief for the Examiner response, and was not in response to the Examiner's response to the arguments in the Appeal Brief. This argument was therefore waived.

CONCLUSIONS OF LAW

The rejection of claims 1–4 and 9–11 under 35 U.S.C. § 101 as directed to non-statutory subject matter is proper.

The rejection of claims 1–4 and 9–11 under 35 U.S.C. § 103(a) as unpatentable over Gupta, Singhal, and Hall is proper.

DECISION

The rejections of claims 1–4 and 9–11 are affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 1.136(a)(1)(iv) (2011).

AFFIRMED